附件2

工业控制系统信息安全自查情况表

**（企业登录平台填报）**

|  |
| --- |
| **一、工业企业基本情况** |
| 单位信息 | 企业名称 |   | 法人代表 |   |
| 单位地址 |  省 市 县（区） |
| 单位网址 |   |
| 行业1 |   | 上一年度销售收入 |   |
| 经济类型 | □ 国有事业单位2 |
| □ 国有及国有控制企业3 （□ 中央 □ 地方） |
| □ 股份制企业 □ 外商及港澳台投资企业4 |
| □ 集体企业 □ 民营企业 |
| □ 其他：  |
| 企业自查联系人 | 姓名 |   | 职务 |   |
| 电话 |   | 部门 |   |
| 工控安全分管领导 | 姓名 |   | 职务 |  |
| 电话 |   | 部门 |  |
| **二、自查情况** |
| **（一）工控系统基本情况** |
| IP地址 | 1.  |
| ... |
| 系统编号 | 系统名称 | 系统简介（系统功能/网络架构） | 数量（套） |
| 1  |  |   |  |
| ... |  |   |  |
| 工业控制系统总数量 |  （套） |
| **（二）工控系统构成情况** |
| 类型 | 设备 | 国内/国外品牌 | 品牌名称 | 数量（台/套） |
| 工业生产控制设备 | 可逻辑编程控制器（PLC） | ○国内 ○国外 |  |  |
| 分布式控制系统（DCS） | ○国内 ○国外 |  |  |
| 远程终端设备（RTU） | ○国内 ○国外 |  |  |
| 数控机床 | ○国内 ○国外 |  |  |
| 工业机器人 | ○国内 ○国外 |  |  |
| 智能仪表 | ○国内 ○国外 |  |  |
| 其 它 | ○国内 ○国外 |  |  |
| 工业网络通信设备 | 工业交换机 | ○国内 ○国外 |  |  |
| 工业路由器 | ○国内 ○国外 |  |  |
| 串口服务器 | ○国内 ○国外 |  |  |
| 其 它 | ○国内 ○国外 |  |  |
| 工业主机设备 | 工业主机5 | ○国内 ○国外 |  |  |
| 组态软件&数据采集与监控系统（SCADA）软件 | ○国内 ○国外 |  |  |
| 工业数据库 | ○国内 ○国外 |  |  |
| 其 它 | ○国内 ○国外 |  |  |
| 工业生产信息系统 | 制造执行系统（MES） | ○国内 ○国外 |  |  |
| ERP管理系统 | ○国内 ○国外 |  |  |
| 工业云 | ○国内 ○国外 |  |  |
| 其 它 | ○国内 ○国外 |  |  |
| 工业网络安全设备 | 工业防火墙 | ○国内 ○国外 |  |  |
| 工业网闸 | ○国内 ○国外 |  |  |
| 主机外设统一管理设备 | ○国内 ○国外 |  |  |
| 网络安全监测设备 | ○国内 ○国外 |  |  |
| 深度包分析和过滤功能的防护设备 | ○国内 ○国外 |  |  |
| 主机安全防护设备 | ○国内 ○国外 |  |  |
| 其 它 | ○国内 ○国外 |  |  |
| **（三）工控系统防护情况** |
| 检查内容 | 执行情况 |
| 安全软件选择与管理情况 | 1、安装防病毒软件或应用程序白名单软件 | 是， （套）; 否， （套） |
| 2、病毒库或白名单规则及时更新 | 是， （套）; 否， （套） |
| 3、定期对工业控制系统进行查杀 | 是， （套）; 否， （套） |
| 4、已建立防病毒和恶意软件入侵管理机制 | 是， （套）; 否， （套） |
| 配置和补丁管理情况 | 1、已建立工业控制网络安全配置策略 | 是， （套）; 否， （套） |
| 2、已建立工业主机安全配置策略 | 是， （套）; 否， （套） |
| 3、已建立工业控制设备安全配置策略 | 是， （套）; 否， （套） |
| 4、已建立工业控制系统配置清单 | 是， （套）; 否， （套） |
| 5、定期对配置清单进行更新和维护 | 是， （套）; 否， （套） |
| 6、及时修复重大工控安全相关漏洞和可能影响工控安全的主机软硬件漏洞 | 是， （套）; 否， （套） |
| 边界安全防护情况 | 1、直接与企业网连接 | 是， （套）; 否， （套） |
| 2、直接与互联网连接 | 是， （套）; 否， （套） |
| 3、对工业控制系统进行安全区域划分 | 是， （套）; 否， （套） |
| 4、对工业控制系统安全区域实施逻辑隔离 | 是， （套）; 否， （套） |
| 物理和环境安全防护情况 | 1、已明确划分重点物理安全防护区域并建立物理安全防护措施 | 是， （套）; 否， （套） |
| 2、拆除或封闭工业主机上不必要外设接口 | 是， （套）; 否， （套） |
| 3、使用外设安全管理技术手段管理外设接口 | 是， （套）; 否， （套） |
| 身份认证情况 | 1、使用身份认证管理手段 | 是， （套）; 否， （套） |
| 2、以最小特权原则分配账户权限 | 是， （套）; 否， （套） |
| 3、未使用默认口令或弱口令 | 是， （套）; 否， （套） |
| 4、定期更新口令 | 是， （套）; 否， （套） |
| 远程访问安全情况 | 1、面向互联网开通HTTP、FTP等网络服务 | 是， （套）; 否， （套） |
| 2、使用数据单向访问控制等策略进行安全加固 | 是， （套）; 否， （套） |
| 3、使用VPN等远程接入方式 | 是， （套）; 否， （套） |
| 4、保留工业控制系统相关访问日志 | 是， （套）; 否， （套） |
| 安全监测情况 | 1、在工业控制网络部署网络安全监测设备 | 是， （套）; 否， （套） |
| 2、在重要工业控制设备前端已部署具备深度包分析和过滤功能防护设备 | 是， （套）; 否， （套） |
| 资产安全情况 | 1、建立工业控制系统资产清单 | 是， （套）; 否， （套） |
| 2、对关键主机设备进行冗余配置 | 是， （套）; 否， （套） |
| 3、对网络设备进行冗余配置 | 是， （套）; 否， （套） |
| 4、对控制组件进行冗余配置 | 是， （套）; 否， （套） |
| 数据安全情况 | 1、对静态存储的重要工业数据进行保护 | 是， （套）; 否， （套） |
| 2、对动态传输的重要工业数据进行保护 | 是， （套）; 否， （套） |
| 3、定期备份关键业务数据 | 是， （套）; 否， （套） |
| 4、对测试数据进行保护 | 是， （套）; 否， （套） |
| 供应链管理情况 | 1、合同中已约定服务商在服务过程中应当承担的信息安全责任和义务 | 是， （套）; 否， （套） |
| 2、与服务商签订保密协议 | 是， （套）; 否， （套） |
| 应急预案演练情况 | 1、已制定工控安全事件应急响应预案 | ○是; ○否 |
| 2、定期对应急预案进行演练 | ○是; ○否 |
| 3、对应急响应预案进行修订 | ○是; ○否 |
| 落实责任情况 | 1、建立工控安全管理机制 | ○是; ○否 |

注1：按照《国民经济行业分类》（GB/T4754-2017）规定填写。
注2：按照《事业单位登记管理暂行条例》登记的，为社会公益目的、由国家机关举办或者其他组织组织利用国有资产举办的，从事教育、科技、文化、卫生等活动的社会服务组织。
注3：按照《中华人民共和国企业法人登记管理条例》登记注册的三类经济组织：（1）全部资产归国家所有的（非公司制）国有企业；（2）全部资产归国家所有的国有独资有限责任公司；（3）由国有资本占控制地位的有限责任公司和股份有限公司，此处称国有控股公司。
注4：包括港、澳、台资本和其他地区外资资本投资设立的独资或控股的独资公司、有限责任公司和股份有限公司。

注5：工业主机是指工业生产控制各业务环节涉及组态、操作、监控、数据采集与存储等功能的主机设备载体，包括工程师站、操作员站、历史站等。